UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,470	11/24/1999	Akito Niwa	04329.2191	5068

22852 7590 09/18/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	6

DATE MAILED: 09/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/448,470	NIWA ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7 and 8* is/are rejected.

7)☒ Claim(s) *6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 November 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. **Claims 1-8** have been examined.

Information Disclosure Statement PTO-1449

2. The pages of the all references submitted by applicant have been considered.

Drawings

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description Page 8, line 15; items "19". Correction is required.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: "11" in fig. 2; "w8" in fig. 9; "x3" in fig.12. Correction is required.

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "1" in fig. 1, 7, 10 has been used to designate "user #1"", "user #2" and "user #3". Examiner suggests Applicant use different numbering for each user in the drawings and corresponding descriptions in the specification; reference character "13" in fig.2 has been used to designate both "CPU" and "Controller". Correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

7. Claims 1-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claims 1-8, the "means for..", "information for..", "the key for..", "approval for.." and "so as to be.." phrases makes the claims indefinite and unclear in that neither means nor interrelationship of means are set forth in these claims in order to achieve the desired results expressed in the "means for..", "information for..", "the key for..", "approval for.." and "so as to be.." phrases.

In claims 1-8, the "means for..", "information for..", "the key for..", "approval for.." and "so as to be.." phrases makes the claims indefinite and unclear in that neither method steps nor interrelationship of method steps are set forth in these claims in order to achieve the desired results expressed in the "means for..", "information for..", "the key for..", "approval for.." and "so as to be.." phrases.

In claims 2, 5 and 6, the "wherein.." phrases makes the claims indefinite and unclear in that neither means nor interrelationship of means are set forth in these claims in order to achieve the desired results expressed in the "wherein..." phrases.

In claims 2, 5 and 6, the "wherein.." phrases makes the claims indefinite and unclear in that neither method steps nor interrelationship of method steps are set forth in these claims in order to achieve the desired results expressed in the "wherein..." phrases.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) do not apply to the examination of this application as the application being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

9. **Claims 1-2 and 7-8** are rejected under 35 U.S.C. 102(e) as being anticipated by Gennaro et al (5,937,066A).

As per claims 1-2 and 7-8 Gennaro et al (5,937,066A) teach an encryption apparatus, a cryptographic communication system and a computer-readable storage medium storing a program comprising: means for encrypting a data body (see fig.2, item 34); and means for transmitting transmission data to a receiver (see fig.1-2 and fig.3 transmission between sender and receiver), the transmission data including: the encrypted data body (see fig.2, item 134); sender's key recovery data obtained by encrypting recovery information for recovering a key for decrypting the encrypted data body to allow a key recovery agent registered by a sender to decrypt the recovery information (see fig.3-5; abstract; col.4, lines 66-67; col.5, lines 1-10 and 24-44); and receiver's key recovery data obtained by encrypting the recovery information for recovering the key for decrypting the encrypted data body to allow a key recovery agent registered by a receiver to decrypt the recovery information (see col.5, lines 45-67; col.6, lines 1-38); and wherein the decryption of the key is being done by plurality of the recovery agent as recited in claim 2 (see fig.1, item 112 and 114; fig.4; col.15, lines 37-56 where the recovery agent 1 and 2 are involved in decryption) and wherein all recovery agents are approved and authorized by an authorized party as recited in claim 7 (see fig.3 and 9; col.15, lines 27-37 wherein the third authorized party or the approver is a service provider or law enforcement agency and authentication of the agent is being done in fig.9 based on agent id).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 3-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro et al (5,937,066A) in view of Micali (5,276,737 A).

As per claims 3 Gennaro et al (5,937,066A) teach an encryption apparatus, a cryptographic communication system and a computer-readable storage medium storing a program comprising: means for encrypting a data body (see fig.2, item 34); and means for transmitting transmission data to a receiver (see fig.1-2 and fig.3 transmission between sender and receiver), the transmission data including: the encrypted data body (see fig.2, item 134); sender's key recovery data obtained by encrypting recovery information for recovering a key for decrypting the encrypted data body to allow a key recovery agent registered by a sender to decrypt the recovery information (see fig.3-5; abstract; col.4, lines 66-67; col.5, lines 1-10 and 24-44); and receiver's key recovery data obtained by encrypting the recovery information for recovering the key for decrypting the encrypted data body to allow a key recovery agent registered by a receiver to decrypt the recovery information (see col.5, lines 45-67; col.6, lines 1-38); and wherein the decryption of the key is being done by plurality of the

recovery agent (see fig.1, item 112 and 114; fig.4; col.15, lines 37-56 where the recovery agent 1 and 2 are involved in decryption) and wherein all recovery agents are approved and authorized by an authorized party (see fig.3 and 9; col.15, lines 27-37 wherein the third authorized party or the approver is a service provider or law enforcement agency and authentication of the agent is being done in fig.9 based on agent id) but do not disclose sender's or receiver's key comprised of a plurality of key pieces obtained by dividing the key into pieces. However Micali (5,276,737 A) teach senders or receiver's key comprised of a plurality of key pieces obtained by dividing the key into pieces (see abstract and also see Gennaro's col.6, lines 40-48 with respect to Micali's teaching). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Micali's key dividing and sharing in Gennaro's key recovery system and method in order to have multiple phase cryptographic key recovery system by plurality of approved recovery agent to reconstruct the decryption encryption key.

As per claim 5 Gennaro et al (5,937,066A) teach a cryptographic communication system according to claim 3, further comprising:

An approver apparatus for approving a requester for key recovery agent registration approval and approving an authorized third party, who requests an approval for decrypting the sender's or receiver's key recovery data only when a request is made by a party approved by an approver (see fig.3 and 9; col.15, lines 27-37 wherein the third

authorized party or the approver is a service provider or law enforcement agency and authentication of the agent is being done in fig.9 based on agent id).

As per claim 4 Gennaro et al (5,937,066A) teach a cryptographic communication system according to claim 3, further comprising: a certificate authority apparatus arranged to allow accepting registration of at least key recovery agent and receivers and provide information representing correspondence between each registered receiver and a key recovery agent and information representing that said encryption apparatus encrypts the recovery information so as to allow the key recovery agent to decrypt the recovery information (see col.5, lines 45-67; col.6, lines 1-38 and wherein the decryption of the key is being done by plurality of the recovery agent as disclosed in fig.1, item 112 and 114; fig.4; col.15, lines 37-56 where the recovery agent 1 and 2 are involved in decryption)

Allowable Subject Matter

12. Claim 6 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S.Patent No. US (5,796,830 A) teach interoperable cryptographic key recovery system.

U.S.Patent No. US (6,249,585 B1) teach publicly verifiable key recovery.

U.S.Patent No. US (6,335,972 B1) teach framework-based cryptographic key recovery system.

U.S.Patent No. US (6,052,496 A) teach interoperable cryptographic key recovery system with verification by comparison.

U.S.Patent No. US (6,058,188 A) teach method and apparatus for interoperable validation of key recovery information in a cryptographic system.

U.S.Patent No. US (5,315,658 A) teach fair cryptosystems and methods of use.

U.S.Patent No. US (5,907,618 A) teach method and apparatus for verifiably providing key recovery information in a cryptographic system.

U.S.Patent No. US (5,815,573 A) teach cryptographic key recovery.

U.S.Patent No. US () teach

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

After-Final	(703) 746-7238
Official	(703) 872-9306
Non-Official/Draft	(703) 746-7240

Kambiz Zand
09/10/03

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100